

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11102333 A

(43) Date of publication of application: 13 . 04 . 99

(51) Int. Cl

G06F 13/00

G06F 13/00

G06F 9/06

(21) Application number: 09260262

(22) Date of filing: 25 . 09 . 97

(71) Applicant:

FUJITSU LTD

(72) Inventor:

ISHIDERA NOBUTAKA
SATOU SHIYUUKO

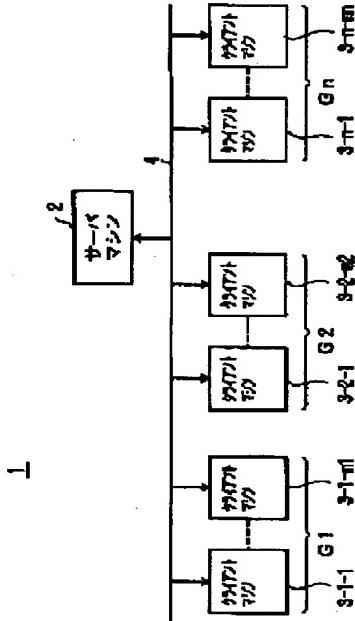
(54) TERMINAL MANAGING METHOD, MANAGING DEVICE, AND TERMINAL DEVICE, COMPUTER SYSTEM USING THE SAME, AND RECORDING MEDIUM WHERE PROGRAM IMPLEMENTING THEM IS RECORDED

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a terminal managing method which can surely make and control a computer virus check on respective information processors connected to a network in network environment.

SOLUTION: A computer virus check request which initiates computer virus check programs of clients 3-1-1 to 3-1-m1, 3-2-1 to 3-2-m2... and 3-n-1 to 3-n-mn to is sent from a server machine to the network 4 and the clients 3-1-1 to 3-1-m1, 3-2-1 to 3-2-m2... and 3-n-1 to 3-n-mn starts the computer virus check programs at the computer virus check request from the server machine 2 to make computer virus checks.

COPYRIGHT: (C)1999,JPO



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-102333

(43)公開日 平成11年(1999)4月13日

(51)Int.Cl.^a
G 0 6 F 13/00
9/06

識別記号
3 5 1
3 5 4
5 5 0

F I
G 0 6 F 13/00
9/06

3 5 1 Z
3 5 4 Z
5 5 0 Z

審査請求 未請求 請求項の数26 O L (全 22 頁)

(21)出願番号 特願平9-260262

(22)出願日 平成9年(1997)9月25日

(71)出願人 000005223

富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 石寺 紳高
東京都稻城市大字大丸1405番地 株式会社
富士通パソコンシステムズ内

(72)発明者 佐藤 周子
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 弁理士 伊東 忠彦

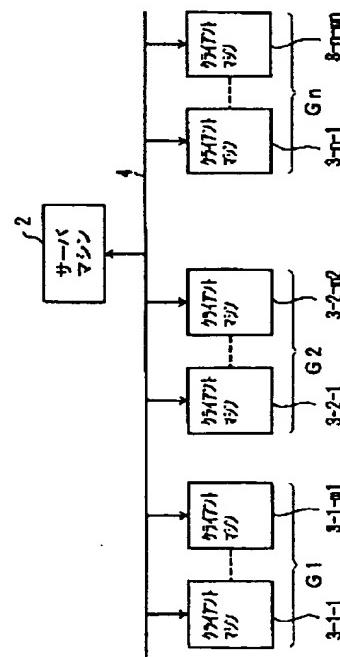
(54)【発明の名称】 端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体

(57)【要約】 (修正有)

【課題】 ネットワーク環境下でネットワークに接続された各情報処理装置のコンピュータウィルスチェックを確実に実行、管理できる端末管理方法を提供する。

【解決手段】 サーバマシン2によりクライアント3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn のコンピュータウィルスチェック要求をネットワーク4に送信し、クライアント3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn によりサーバマシン2からのコンピュータウィルスチェック要求に応じてコンピュータウィルスチェックプログラムを起動し、コンピュータウィルスチェックを実行する。

本発明の第1実施例のシステム構成図



【特許請求の範囲】

【請求項1】 コンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置と管理装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信し、前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動し、コンピュータウィルスチェックを実行することを特徴とする端末管理方法。

【請求項2】 前記管理装置は、前記コンピュータウィルスチェック要求を、前記複数の端末装置のうち予め設定された所望の端末装置に供給することを特徴とする請求項1記載の端末管理方法。

【請求項3】 前記端末装置は、前記管理装置から供給される前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段で実行されたコンピュータウィルスチェック結果を前記管理装置に送信し、前記管理装置は、前記端末装置から送信された前記コンピュータウィルスチェック結果を一括管理することを特徴とする請求項1又は2記載の端末管理方法。

【請求項4】 前記管理装置は、前記複数の端末装置から送信された前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信することを特徴とする請求項3記載の端末管理方法。

【請求項5】 前記管理装置は、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止することを特徴とすることを特徴とする請求項1乃至4のいずれか一項記載の端末管理方法。

【請求項6】 前記管理装置は、前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することを特徴とする請求項1乃至5のいずれか一項記載の端末管理方法。

【請求項7】 管理装置と、複数の端末装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、前記管理装置は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段を備えるとともに、コンピュータウィルスチェック要求を前記複数の端末装置に送信し、前記複数の端末装置は、前記管理装置から送信された前記コンピュータウィルスチェック要求に応じて前記管理装置の前記コンピュータウィルスチェック手段にアクセス

し、自装置に対するコンピュータウィルスチェックを実行することを特徴とする端末管理方法。

【請求項8】 前記管理装置は、前記コンピュータウィルスチェック要求を前記複数の端末装置のうち予め設定された所望の端末装置に供給することを特徴とする請求項7記載の端末管理方法。

【請求項9】 前記端末装置は、前記管理装置の前記コンピュータウィルスチェック手段を起動することにより得られるコンピュータウィルスチェック結果を前記管理装置に送信し、

前記管理装置は、前記端末装置から送信されたコンピュータウィルスチェック結果を管理情報として一括管理することを特徴とする請求項7又は8記載の端末管理方法。

【請求項10】 前記管理装置は、前記複数の端末装置から送信されたコンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信することを特徴とする請求項9記載の端末管理方法。

【請求項11】 前記管理装置は、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止することを特徴とする請求項7乃至10のいずれか一項記載の端末管理方法。

【請求項12】 コンピュータウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続される管理装置であって、前記コンピュータウィルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手段と、前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手段とを備えることを特徴とする管理装置。

【請求項13】 前記コンピュータウィルスチェック要求を、前記複数の端末装置のうちいずれの端末装置に送信するかを指定する指定手段を備え、

前記指定手段により指定された端末装置に対して前記コンピュータウィルスチェック要求を送信することを特徴とする請求項12記載の管理装置。

【請求項14】 前記送信した前記コンピュータウィルスチェック要求に応じて前記端末装置で行われたコンピュータウィルスチェック結果を受信する受信手段と、前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を管理する管理手段とを備えることを特徴とする請求項12または13記載の管理装置。

【請求項15】 前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された端末装置に送信する送信するこ

とを特徴とする請求項14記載の管理装置。

【請求項16】 前記複数の端末装置の接続状態を監視する監視手段と、

前記複数の端末装置のうち所定期間接続されていない端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与する情報付与手段と、

前記情報が付与された端末装置には前記コンピュータウィルスチェック要求の送信を停止する送信停止手段とを備えることを特徴とする請求項12乃至15のいずれか一項記載の管理装置。

【請求項17】 前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信するコンピュータウィルスパターン送信手段を備えることを特徴とする請求項12乃至16のいずれか一項記載の管理装置。

【請求項18】 ネットワークを介して管理装置に接続される端末装置であって、

前記管理装置からのコンピュータウィルスチェック要求を受信する手段と、

前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する起動手段と、コンピュータウィルスのチェックを実行するチェック実行手段とを備えることを特徴とする端末装置。

【請求項19】 前記受信したコンピュータウィルスチェック要求に応じて実行したコンピュータウィルスチェックの結果を前記管理装置に送信する送信手段を備えることを特徴とする請求項18記載の端末装置。

【請求項20】 前記コンピュータウィルスチェック要求とともにコンピュータウィルスパターンを受信し、該コンピュータウィルスパターンを用いてウィルスのチェックを行うことを特徴とする請求項18または19記載の端末装置。

【請求項21】 ネットワークを介して管理装置に接続される端末装置であって、

前記管理装置からのコンピュータウィルスチェック要求を受信する受信手段と、

前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、自装置に対するコンピュータウィルスチェックを実行する手段とを備えることを特徴とする端末装置。

【請求項22】 コンピュータウィルスをチェックするコンピュータウィルスチェック手段を具备する複数の端末装置と管理装置とがネットワークを介して接続されたコンピュータシステムにおいて、

前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、

前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック起動手段を備えることを特徴とするコンピュータシステム。

【請求項23】 管理装置と複数の端末装置とがネットワークを介して接続されたコンピュータシステムにおいて、

前記管理装置は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段と、

コンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、

前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記管理装置の前記コンピュータウィルスチェック手段にアクセスするアクセス手段と、

自装置に対するコンピュータウィルスチェックを実行するコンピュータウィルスチェック実行手段とを備えることを特徴とするコンピュータシステム。

【請求項24】 ウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続されるコンピュータに、前記コンピュータウィルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手順と、前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手順とを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項25】 ネットワークを介して管理装置に接続されるコンピュータに、

前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する手順と、コンピュータウィルスのチェックを実行する手順とを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項26】 ネットワークを介して管理装置に接続されるコンピュータに、

前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、該コンピュータウィルスチェック手段を起動する手順と、

前記起動されたコンピュータウィルスチェック手段により自装置に対するコンピュータウィルスチェックを実行する手順とを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体に係り、特に、ネットワークに接続された複数の端末装置をネットワークに接続された管理装置により一括して管理する端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体に関する。

【0002】近年、情報処理装置などでは、コンピュータウィルス種の増加に伴い、ウィルスチェックは欠かすことができない。特に、ネットワーク環境においては、コンピュータウィルスへの感染はネットワーク下の全ての情報処理装置に影響があるので、定期的なコンピュータウィルスチェックが欠かせない。このため、ネットワーク環境下にネットワークに接続された端末装置（情報処理装置）のコンピュータウィルスチェックの状態をネットワーク管理者などが一括して管理している。

【0003】しかし、各端末装置でのコンピュータウィルスチェックの実行は、人為的であり、計画的な運用管理が行えない。

【0004】

【従来の技術】従来のネットワーク環境下の情報処理装置ではコンピュータウィルスのチェックは、各情報処理装置に記憶されたコンピュータウィルスチェックプログラムを各情報処理装置のそれぞれで、その情報処理装置を使用するユーザ自身が任意に起動することで実行されている。

【0005】

【発明が解決しようとする課題】しかるに、従来のネットワーク環境下でのコンピュータウィルスチェック方法は、各情報処理装置にコンピュータウィルスチェックプログラムを格納しておき、各情報処理装置毎に情報処理装置の使用者がコンピュータウィルスプログラムを起動して、コンピュータウィルスチェックを行い、口頭や電子メールなどによりネットワーク管理者に報告していたため、人為的な要素が多く、ウィルスチェックを確実に行えなく、また、運用管理も容易でない等の問題点があった。

【0006】本発明は上記の点に鑑みてなされたもので、ネットワーク環境下でネットワークに接続された各情報処理装置のコンピュータウィルスチェックを確実に実行、管理できる端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の請求項1は、ファイル中のコンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置

と該複数の端末装置のコンピュータウィルスチェックを管理する管理装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信し、前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動し、コンピュータウィルスチェックを実行することを特徴とする。

【0008】請求項1によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができる、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【0009】請求項2は、前記管理装置を、前記コンピュータウィルスチェック要求を、前記複数の端末装置のうち予め設定された所望の端末装置に供給する構成としてなる。請求項2によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるために、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる。

【0010】請求項3は、前記端末装置を、前記管理装置から供給される前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段で実行されたコンピュータウィルスチェック結果を前記管理装置に送信し、前記管理装置を、前記端末装置から送信された前記コンピュータウィルスチェック結果を一括管理する構成としてなる。

【0011】請求項3によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる。請求項4は、前記管理装置を、前記複数の端末装置から送信された前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信する構成としてなる。

【0012】請求項4によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックでき

る。

【0013】請求項5は、前記管理装置を、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止する構成としてなる。請求項5によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる。

【0014】請求項6は、前記管理装置を、前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信する構成としてなる。請求項6によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる。

【0015】請求項7は、ファイル中のコンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する管理装置と、該管理装置によりコンピュータウィルスチェックが管理される複数の端末装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、前記管理装置は、前記コンピュータウィルスチェック要求を前記複数の端末装置に送信し、前記複数の端末装置は、前記管理装置から送信された前記コンピュータウィルスチェック要求に応じて前記管理装置に記憶された前記コンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することを特徴とする。

【0016】請求項7によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定さえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【0017】請求項8は、前記管理装置を、前記コンピュータウィルスチェック要求を前記複数の端末装置のうち予め設定された所望の端末装置に供給する構成として

なる。請求項8によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる。

【0018】請求項9は、前記端末装置を、前記管理装置から供給される前記コンピュータウィルスチェック手段を起動することにより得られるコンピュータウィルスチェック結果を前記管理装置に送信し、前記管理装置は、前記端末装置から送信されたコンピュータウィルスチェック結果を管理情報として一括管理する構成となる。

【0019】請求項9によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を一括してチェックできる。請求項10は、前記管理装置を、前記複数の端末装置から送信されたコンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信する構成となる。

【0020】請求項10によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出し、複数の端末装置のコンピュータウィルスへの感染をチェックできる。

【0021】請求項11は、前記管理装置を、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止する構成としてなる。請求項11によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる。

【0022】請求項12は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続される管理装置であって、前記コンピュータウィルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手段と、前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手段とを備えることを特徴とする。

【0023】請求項12によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコン

ピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【0024】請求項13は、前記コンピュータウィルスチェック要求を、前記複数の端末装置のうちいずれの端末装置に送信するかを指定する指定手段を備え、前記指定手段により指定された端末装置に対して前記コンピュータウィルスチェック要求を送信することを特徴とする。請求項13によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる。

【0025】請求項14は、前記送信した前記コンピュータウィルスチェック要求に応じて前記端末装置で行われたコンピュータウィルスチェック結果を受信する受信手段と、前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を管理する管理手段とを備えることを特徴とする。

【0026】請求項14によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる。請求項15は、前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された端末装置に送信する送信することを特徴とする。

【0027】請求項15によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる。

【0028】請求項16は、前記複数の端末装置の接続状態を監視する監視手段と、前記複数の端末装置のうち所定期間接続されていない端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与する情報付与手段と、前記情報が付与された端末装置には前記コンピュータウィルスチェック要求の送信を停止する送信停止手段とを備えることを特徴とする。

【0029】請求項16によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行

われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる。請求項17は、前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信するコンピュータウィルスパターン送信手段を備えることを特徴とする。

【0030】請求項17によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる。

【0031】請求項18は、ネットワークを介して管理装置に接続される端末装置であって、前記管理装置からのコンピュータウィルスチェック要求を受信する手段と、前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する起動手段と、コンピュータウィルスのチェックを実行するチェック実行手段とを備えることを特徴とする。

【0032】請求項18によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【0033】請求項19は、前記受信したコンピュータウィルスチェック要求に応じて実行したコンピュータウィルスチェックの結果を前記管理装置に送信する送信手段を備えることを特徴とする。請求項19によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる。

【0034】請求項20は、前記コンピュータウィルスチェック要求とともにコンピュータウィルスパターンを受信し、該コンピュータウィルスパターンを用いてウィルスのチェックを行うことを特徴とする。請求項20によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウイ

11

ルスチェックを行うことができる。

【0035】請求項21は、ネットワークを介して管理装置に接続される端末装置であつて、前記管理装置からのコンピュータウィルスチェック要求を受信する受信手段と、前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、自装置に対するコンピュータウィルスチェックを実行する手段とを備えることを特徴とする。

【0036】請求項21によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【0037】請求項22は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置と管理装置とがネットワークを介して接続されたコンピュータシステムにおいて、前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック起動手段を備えることを特徴とする。

【0038】請求項22によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【0039】請求項23は、管理装置と複数の端末装置とがネットワークを介して接続されたコンピュータシステムにおいて、前記管理装置は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段と、コンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記管理装置の前記コンピュータウィルスチェック手段にアクセスするアクセス手段と、自装置に対するコンピュータ

12

ウィルスチェックを実行するコンピュータウィルスチェック実行手段とを備えることを特徴とする。

【0040】請求項23によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【0041】請求項24は、ウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続されるコンピュータに、前記コンピュータウィルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手順と、前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手順とを実行させるためのプログラムを記録媒体に記録することを特徴とする。

【0042】請求項24によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【0043】請求項25は、ネットワークを介して管理装置に接続されるコンピュータに、前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する手順と、コンピュータウィルスのチェックを実行する手順とを実行させるためのプログラムをコンピュータ読み取り可能な記録媒体に記録したことを特徴とする。

【0044】請求項25によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【0045】請求項26は、ネットワークを介して管理装置に接続されるコンピュータに、前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、

50

前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、該コンピュータウィルスチェック手段を起動する手順と、前記起動されたコンピュータウィルスチェック手段により自装置に対するコンピュータウィルスチェックを実行する手順とを実行させるためのプログラムをコンピュータ読み取り可能な記録媒体に記録したことを特徴とする。

【0046】請求項26によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【0047】

【発明の実施の形態】図1に本発明の第1実施例のシステム構成図を示す。本実施例のネットワークシステム1は、サーバマシン2とクライアントマシン3-1-1～3-n-mとがネットワーク4を介して接続されている。ここで、まず、サーバマシン2の構成を図面とともに説明する。

【0048】図2に本発明の第1実施例のサーバマシンのブロック構成図を示す。サーバマシン2は、ネットワーク4との通信を制御する通信制御部11、クライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2・・・3-n-1～3-n-mnに供給すべき情報等がファイルされたファイル装置12、ファイル装置12に情報を書き込むとともにファイル装置12から情報を読み出す制御を行う入出力コントローラ13、ファイル装置12のプログラム領域に格納されたコンピュータウィルスチェック要求プログラムに応じて処理を行なうCPU14、CPU14の作業領域となるRAM15、処理結果を表示するディスプレイ16、ディスプレイ16を制御する表示コントローラ17、コマンド、データを入力するキーボード18、キーボード18の入力を制御するキーボードコントローラ19、通信制御部11、入出力コントローラ13、CPU14、RAM15、表示コントローラ17、キーボードコントローラ19を接続するバス20から構成される。

【0049】通信制御部11はネットワーク2に接続され、クライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2・・・3-n-1～3-n-mnとの接続を行う。ファイル装置12は、データが格納されるデータ領域12a、サーバマシン2で実行される

プログラムが格納されたプログラム領域12b、コンピュータウィルスチェック要求プログラム実行時のタイミングを制御するデータが格納されたコンピュータウィルスチェック要求スケジュール領域12c、コンピュータウィルスチェック結果処理プログラム実行時にクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2・・・3-n-1～3-n-mnから供給されたコンピュータウィルスチェック結果を保持する結果累積領域12dから構成される。

【0050】上記のコンピュータウィルスチェック要求プログラム、コンピュータウィルスチェック結果処理プログラムなどのプログラムやデータは、通信制御部を介して、または図示しないCD-ROMやフロッピディスクなどの可搬型記録媒体に記録されたものを読み取られ、上記ファイル装置12のプログラム領域12aやスケジュール領域12cに格納される。そして、それらはプログラムの実行時に作業領域であるRAM15に格納され、CPU14はそれらプログラムに応じて所定の処理を実行する。

【0051】図3に本発明の第1実施例のコンピュータウィルスチェック要求スケジュールのデータ構成図を示す。サーバマシン2は、クライアントマシン3-1-1～3-n-mnを複数のグループG1～Gnに分割して管理している。ここで、図1に示すようにグループG1は、クライアントマシン3-1-1～3-1-m1、グループG2は、クライアントマシン3-2-1～3-2-m2・・・、グループGnは、クライアントマシン3-n-1～3-n-mnから構成される。

【0052】コンピュータウィルスチェック要求スケジュール領域12cは、グループG1～Gn毎に設定される。1グループ分のコンピュータウィルスチェック要求スケジュール12cは、主に、スケジュールを設定するグループG1～Gnの情報を示すグループ情報ヘッダ領域、グループ情報ヘッダ領域で設定されたグループに属するメンバ(クライアントマシン)の情報を示すメンバ情報領域、1グループの情報の終了を示すグループ情報エンダ領域から構成される。

【0053】また、グループ情報ヘッダ領域は、スケジュールを設定するグループG1～Gnを識別するためのグループID領域、コンピュータウィルスチェック要求を発行すべき日時を設定するための発行日時情報領域、グループの管理者のメールアドレスを示す管理者メールアドレス領域、グループに属するクライアントマシンの数が設定されるメンバ数領域、コンピュータウィルスチェックに用いられるコンピュータウィルスチェックプログラムのバージョンを示すバージョン情報領域から構成される。

【0054】また、メンバ情報領域は、コンピュータウィルスチェックを行うクライアントマシンを識別するためのメンバID領域、コンピュータウィルスチェックを

行うクライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ を使用する人の名前などを設定するメンバ名、コンピュータウイルスチェックを行うクライアントマシンを使用する人のメールアドレスを設定するメンバメールアドレス領域、コンピュータウイルスのチェック結果を通知する先のアドレスを設定するための結果通知先アドレス領域、1メンバ情報の終了を示すエンダ領域から構成される。上記メンバ情報領域がメンバ数分だけ繰り返され、最後にエンダが付与されて、1グループ情報領域とされる。

【0055】サーバマシン2は、上記チェック要求スケジュール12cを監視しており、現在時刻がチェック要求スケジュール管理12cの発行日時情報領域に設定された発行日時になったとき、後述するようにチェック要求スケジュール12cに設定された情報に基づいてコンピュータウイルスチェックの要求を行う。図4に本発明の第1実施例の集計結果累積領域のデータ構成図を示す。

【0056】集計結果累積領域12dは、クライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ を識別するためのメンバIDが格納されるメンバID領域、メンバID領域に格納されたメンバIDを使用する人に名前などのメンバ名が格納されるメンバ名領域、メンバID領域に格納されたメンバIDのクライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ でのコンピュータウイルスチェック結果、及び、コンピュータウイルスチェックに用いられたコンピュータウイルスチェックプログラムのバージョン情報が格納される結果格納領域から1メンバ分の情報が構成される。集計結果累積領域12dは、上記メンバID領域、メンバ名領域、結果格納領域がメンバ数だけ繰り返される。

【0057】サーバマシン2は、コンピュータウイルスチェック要求プログラムによりファイル装置12のコンピュータウイルスチェック要求スケジュール領域12cに予め設定されたスケジュールに応じてクライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ にコンピュータウイルスチェック要求を送信し、コンピュータウイルスチェック結果処理プログラムによりクライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ でのコンピュータウイルスチェック結果を集計して、管理者に送信する。

【0058】次にクライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ の構成を図面とともに説明する。図5に本発明の第1実施例のクライアントマシンのブロック構成図を示す。クライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$

(9) 16
m₁, 3-2-1~3-2-m₂ . . . 3-n-1~3-n-m_n は、ネットワーク4との通信を制御する通信制御部21、データ、プログラムなどが格納されるファイル装置22、ファイル装置22に情報を書き込むとともにファイル装置22から情報を読み出す制御を行う入出力コントローラ23、ファイル装置22のプログラム領域に格納されたコンピュータウイルスチェックプログラムに応じてコンピュータウイルスチェックを実行するCPU24、CPU24の作業領域となるRAM25、

10 処理結果を表示するディスプレイ26、ディスプレイ26を制御する表示コントローラ27、コマンド、データを入力するキーボード28、キーボード28の入力を制御するキーボードコントローラ29、通信制御部21、入出力コントローラ23、CPU24、RAM25、表示コントローラ27、キーボードコントローラ29を接続するバス30から構成される。

【0059】通信制御部21はネットワーク2に接続され、サーバマシン2との接続を制御する。ファイル装置22は、データが格納されるデータ領域22a、クライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ で実行されるプログラムが格納されたプログラム領域22b、コンピュータウイルスチェック結果を格納するコンピュータウイルスチェック結果格納領域22c、コンピュータウイルスチェックプログラム実行時に用いられるコンピュータウイルスパターン領域22dから構成される。

【0060】上記のコンピュータウイルスチェックプログラムなどの本発明に関わるプログラムやウイルスパターンは、通信制御部を介して、または図示しないCD-ROMやフロッピィディスクなどの可搬型記録媒体に記録されてたものを読み取られ、上記ファイル装置22のプログラム領域22bやコンピュータウイルスパターン領域22dに格納される。そして、それらはプログラムの実行時に作業領域であるRAM25に格納され、CPU24はそれらプログラムに応じて所定の処理が実行される。

【0061】図6に本発明の第1実施例のクライアントマシンのコンピュータウイルスチェック結果領域のデータ構成図を示す。クライアントマシン $3-1-1 \sim 3-1-m_1, 3-2-1 \sim 3-2-m_2 \dots 3-n-1 \sim 3-n-m_n$ では、コンピュータウイルスチェックプログラムによるコンピュータウイルスチェック結果を図6に示すようなデータ形式のコンピュータウイルスチェック結果格納領域22cに格納した後、サーバ2に送信する。

【0062】まず、コンピュータウイルスチェック結果格納領域22cは、自装置の属するグループを認識するためのグループIDが格納されるグループID領域、自装置を認識するためのメンバIDが格納されるメンバID領域、ステップS2-2でのコンピュータウイルスチ

エック結果を格納するための結果領域、コンピュータウイルスチェックプログラムで使用したコンピュータウィルスパターンのバージョン情報を格納するためのバージョン情報領域から構成される。

【0063】図7に本発明の第1実施例のクライアントマシンのコンピュータウィルスパターン領域のデータ構成図を示す。クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2...3-n-1~3-n-mnのファイル装置22に設定されたコンピュータウィルスパターンファイル領域22dは、バージョンを識別するためのバージョン情報が格納されたバージョン情報領域、バージョン情報に応じたコンピュータウィルスのパターンが格納されるコンピュータウィルスパターン領域とから構成される。

【0064】クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2...3-n-1~3-n-mnでは、サーバマシン2から供給される自装置へのコンピュータウィルスチェック要求に応じてコンピュータウィルスチェックプログラムが起動し、ファイル装置22に設定されたコンピュータウィルスパターンファイル領域22dのコンピュータウィルスパターンを参照し、ファイル装置22のデータ領域22a、及び、プログラム領域22bに格納されたデータとコンピュータウィルスパターンファイル領域22dのコンピュータウィルスパターンと比較して、一致するパターンを検索し、コンピュータウィルスパターンと一致するデータが存在する場合には、ウィルスが存在すると判断して、ウィルスパターンの除去などを行う。

【0065】次に、サーバマシン2で実行されるコンピュータウィルス要求プログラムの動作を図面と共に説明する。図8に本発明の第1実施例のサーバマシンのコンピュータウィルスチェック要求プログラムの処理フローチャートを示す。サーバマシン2では、コンピュータウィルス要求プログラムにより、まず、図3に示す要求スケジュールを参照して、設定されているメンバ情報を順次取り出す(ステップS1-1, S1-2, S1-3)。

【0066】次に、グループ情報中の発行日時情報領域に格納された発行日時情報を読み出して、現在日時と比較する(ステップS1-4)。ステップS1-4の比較結果、発行日時が現在日時であれば、メンバ情報領域を順に読み出し、各メンバ情報領域のメンバメールアドレス領域に格納されたメンバメールアドレス宛にウィルスチェック要求パケットをネットワーク4に送信する(ステップS1-5, S1-6)。

【0067】クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2...3-n-1~3-n-mnは、ネットワーク4上のパケット監視しており、自装置のパケットのみを受信する。次に、クライアントマシン3-1-1~3-1-m1, 3-2-1~3-

-2-m2...3-n-1~3-n-mnのコンピュータウィルスチェックプログラムの動作を図面と共に説明する。

【0068】図9に本発明の第1実施例のクライアントマシンのコンピュータウィルスチェックプログラムの処理フローチャートを示す。クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2...3-n-1~3-n-mnではサーバマシン2から自装置宛のコンピュータウィルスチェック要求パケットを受信すると、コンピュータウィルスチェックプログラムを起動させる(ステップS2-1)。

【0069】ステップS2-1でコンピュータウィルスチェックプログラムが起動されると、ファイル装置22のデータ領域22a及びプログラム領域22bに格納されたデータを順次読み出し、コンピュータウィルスパターン領域22dのコンピュータウィルスパターンと比較して一致するパターンを検索する。比較結果、コンピュータウィルスパターンと一致するデータが存在する場合には、ウィルスが存在すると判断して、ウィルスパターンの除去などを行うとともに、コンピュータウィルスパターンのバージョン情報、及び、検出したウィルスの情報を保持する。また、比較結果、コンピュータウィルスパターンと一致するデータが存在しない場合には、ウィルスは存在しないと判断して、チェックしたコンピュータウィルスパターンのバージョン情報、及び、ウィルスが存在しない旨の情報を保持する。

【0070】次に、コンピュータウィルスチェックプログラムのチェック結果をサーバへの報告形式にまとめ、ファイル装置22のコンピュータウィルスチェック結果領域22cに格納する(ステップS2-2)。クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2...3-n-1~3-n-mnは、ステップS2-2でのコンピュータウィルスチェックプログラムによるコンピュータウィルスのチェック後、図6に示すように自装置の属するグループID、自装置のメンバID、ウィルスチェック結果、コンピュータウィルスパターンのバージョン情報からなる結果報告情報を含むサーバマシン2宛のパケットを作成して、サーバマシン2に通知する(ステップS2-3)。

【0071】サーバマシン2は、クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2...3-n-1~3-n-mnからコンピュータウィルスのチェック結果を受信すると、コンピュータウィルスチェック結果処理プログラムを実施する。次に、サーバマシン2のコンピュータウィルスチェック結果処理プログラムの動作を図面とともに説明する。

【0072】図10に本発明の第1実施例のサーバマシンのコンピュータウィルスチェック結果処理プログラムの処理フローチャートを示す。サーバマシン2では、クライアントマシン3-1-1~3-1-m1, 3-2-1~3-

1～3～2～m2 … 3～n～1～3～n～mn からコンピュータウィルスのチェック結果パケットを受信すると、コンピュータウィルスチェック結果プログラムが起動し、クライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn から受信したコンピュータウィルスチェック結果をグループ毎にファイル装置12の集計結果累積領域12dに保存する(ステップS3-1)。

【0073】ステップS3-1でコンピュータウィルスチェック結果を保存する際の情報は、グループ毎に保存される。1グループの情報は、図4に示す1メンバの情報が繰り返し、メンバ分だけ順次配列された構成とされている。1メンバ分の情報は、メンバ名、コンピュータウィルスチェック結果、ウィルスチェックパターンのバージョン情報から構成され、これがメンバ数分だけ繰り返したファイルとして保存される。このとき、ファイル名を、例えば、グループID及びコンピュータウィルスチェック日時をアンダーバー記号を介して配列し、ファイル形式(拡張子)を付与したものとすることにより、ファイル名から容易にグループ及びコンピュータウィルスチェック日時を認識できる。

【0074】図6に示すようにクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn からのコンピュータウィルスチェック結果が保存されると、次に、処理結果をコンピュータウィルスチェック要求スケジュール12cのメンバ情報領域の結果通知先アドレス領域に格納されたアドレス宛に送信する(ステップS3-2)。

【0075】ステップS3-2でグループ内の全てのクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn のコンピュータウィルスチェック結果が得られると、次に、保存されたコンピュータウィルスの処理結果でグループ内の全てのクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn からコンピュータウィルスチェック結果が得られていれば(ステップS3-3)、次に、同じグループ内の全てのクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn のコンピュータウィルスチェック結果を一覧にし、図3に示されるコンピュータウィルスチェック要求スケジュール12cのグループ情報ヘッダ領域の管理者メールアドレス領域に格納された管理者メールアドレス宛に送信する(ステップS3-4)。

【0076】図11に本発明の第1実施例のグループ担当者(管理者)に送信するコンピュータウィルスチェック結果一覧のフォーマットを示す。ステップS3-4では、図4に示す集計結果累積領域12dに格納されたクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn のコ

ンピュータウィルスチェック結果からグループ担当者に送信するコンピュータウィルスチェック結果一覧をテキストファイル形式で作成し、管理者に送信する。コンピュータウィルスチェック結果一覧は、図11に示すように、最上段に、グループID、及び、コンピュータウィルスチェックが実施された日時が記録される。図11では、グループIDが「A」、施行日時が「97年7月7日」であることがわかる。

【0077】次の段から順次グループに属するクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn でのコンピュータウィルスチェック結果が記録される。コンピュータウィルスチェック結果を記録する領域には、メンバ名、バージョン情報、コンピュータウィルスチェック結果が記録される。

【0078】図11の上段に記録された領域には、メンバ名「A氏」、バージョン情報「V**L**」であり、コンピュータウィルスチェック結果はコンピュータウィルスが発見できない状態である情報「Normal end」が記録されている。また、図11の下段に記録された領域には、メンバ名「B氏」、バージョン情報「V**L**」であり、コンピュータウィルスチェック結果はコンピュータウィルス「**」が発見され、除去されたことを示す旨の情報が記録される。図11に示すような情報がテキストファイルとして供給される。

【0079】管理者は、図11に示すようなコンピュータウィルスチェック結果一覧を参照して、自分の管理するグループのコンピュータウィルスチェックの結果を認識する。ステップS3-4で、図11に示すようなコンピュータウィルスチェック結果一覧が管理者に送信された後、結果をバックアップとしてファイル装置の結果累積領域に保存する(ステップS3-5)。

【0080】本実施例によれば、ネットワーク4に接続されたクライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn のコンピュータウィルスチェックをサーバ2からの要求により自動で実施できるので、コンピュータウィルスチェックを確実に実施できる。また、コンピュータウィルスチェックは、予め設定されたスケジュールに応じて実施されるため、使用時間を避けて、実際の作業を妨害することなく実施できる。さらに、定期的に実施できるので、有効なコンピュータウィルスチェックを実現できる。

【0081】なお、本実施例では、各クライアントマシン3-1-1～3-1-m1, 3-2-1～3-2-m2 … 3-n-1～3-n-mn にコンピュータウィルスチェックプログラムを搭載したが、コンピュータウィルスパターンは年々増加しており、本実施例の構成ではコンピュータウィルスパターンを更新する場合には、各クライアントマシン3-1-1～3-1-m1, 3-

$-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ の夫々で最新コンピュータウィルスパターンをインストールする必要があり、手間がかかる。また、各クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ のうち、一つのクライアントマシンでも最新コンピュータウィルスパターンのインストールを怠ると、コンピュータウィルスパターンに抜けが生じ、最新のコンピュータウィルスパターンを見逃してしまう。

【0082】そこで、コンピュータウィルスパターンをサーバマシンから供給する構成が考えられる。第2実施例として、コンピュータウィルスパターンをサーバマシンから供給する構成の実施例について説明する。なお、クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ の構成及び動作は第1実施例と同じため、その説明は省略する。

【0083】まず、本実施例のサーバマシン50の構成を図面とともに説明する。図12に本発明の第2実施例のサーバマシンのブロック構成図を示す。同図中、図2と同一構成部分には同一符号を付し、その説明は省略する。本実施例のサーバマシン50は、ファイル装置51のデータ領域52に最新コンピュータウィルスパターンデータ領域52aを有する。最新コンピュータウィルスパターンデータ領域52aには、最新のコンピュータウィルスパターンが格納されている。

【0084】サーバマシン50は、クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ にコンピュータウィルスチェック要求スケジュール12cに基づいて供給するコンピュータウィルスチェック要求の送信時に、コンピュータウィルスチェック要求スケジュール12cに格納された各クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ のコンピュータウィルスパターンのバージョン情報を参照して、最新コンピュータウィルスパターンデータ領域52aに格納された最新コンピュータウィルスパターンのバージョン情報と比較し、クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ のコンピュータウィルスパターンに不足するコンピュータウィルスパターンをコンピュータウィルスチェック要求とともにクライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ に送信する。

【0085】図13に本発明の第2実施例のサーバマシンのコンピュータウィルスチェック要求プログラムの処理フローチャートである。サーバマシン2では、コンピュータウィルス要求プログラムにより、まず、図3に示す要求スケジュールを参照して、設定されているメンバ

情報を順次取り出す（ステップS4-1, S4-2, S4-3）。

【0086】次に、グループ情報中の発行日時情報領域に格納された発行日時情報を読み出して、現在日時と比較する（ステップS4-4）。ステップS4-4の比較結果、発行日時が現在日時であれば（ステップS4-5）、次に、コンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのバージョン情報を参照して、サーバマシン2のファイル装置51のデータ領域52に格納されたコンピュータウィルスパターンデータ52aのバージョン情報を比較する（ステップS4-6）。

【0087】ステップS4-6で、コンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのバージョン情報をサーバマシン2のファイル装置51のデータ領域52に格納されたコンピュータウィルスパターンデータ52aのバージョン情報とが不一致の場合には、ウィルスチェック要求パケットにコンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのコンピュータウィルスパターンに不足するコンピュータウィルスパターン及びバージョン情報を付与して、メンバ情報領域のメンバメールアドレス領域に格納されたメンバメールアドレス宛にウィルスチェック要求パケットをネットワーク4に送信する（ステップS4-7）。

【0088】また、ステップS4-6で、コンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのバージョン情報をサーバマシン2のファイル装置51のデータ領域52に格納されたコンピュータウィルスパターンデータ52aのバージョン情報とが一致する場合には、メンバ情報領域のメンバメールアドレス領域に格納されたメンバメールアドレス宛にウィルスチェック要求パケットだけをネットワーク4を介して送信する（ステップS4-8）。

【0089】クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ は、ネットワーク4上のパケット監視しており、自装置のパケットのみを受信する。このとき、クライアントマシン $3-1-1 \sim 3-1-m_1$, $3-2-1 \sim 3-2-m_2 \cdots 3-n-1 \sim 3-n-m_n$ は、コンピュータウィルスパターンが付与されたコンピュータウィルスチェック要求を受信すると、付与されたコンピュータウィルスパターンをコンピュータウィルスチェックプログラムのコンピュータウィルスパターンに付加するとともに、バージョン情報をコンピュータウィルスチェック要求に付与されたバージョン情報を更新する。

【0090】以下、第1実施例の図9に示すコンピュータウィルスチェックプログラムを実行して、サーバマシン2にコンピュータウィルスチェック結果を送信する。サーバマシン2は、第1実施例の図10に示すコンピュータウィルスチェック結果処理プログラムを実行する。本実施例によれば、クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 … 3-n-1~3-n-mnに格納されたコンピュータウィルスチェックプログラムを常に最新のバージョンのコンピュータウィルスパターンで実行できるので、コンピュータウイルスから確実にシステムを防御できる。

【0091】なお、本実施例では、サーバマシン50からコンピュータウィルスパターンだけを提供する構成としたが、サーバマシンにコンピュータウィルスチェックプログラムを搭載し、コンピュータウィルスチェック時にクライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 … 3-n-1~3-n-mnからアクセスする構成も考えられる。

【0092】第3実施例として、サーバマシン2にコンピュータウィルスチェックプログラムを搭載し、コンピュータウィルスチェック時にクライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 … 3-n-1~3-n-mnからアクセスする実施例について図面とともに説明する。まず、サーバマシンの構成を図面とともに説明する。

【0093】図14に本発明の第3実施例のサーバマシンのブロック構成図を示す。同図中、図2と同一構成部分には同一符号を付し、その説明は省略する。本実施例のサーバマシン110は、ファイル装置111のプログラム領域112にコンピュータウィルスをチェックするコンピュータウィルスチェックプログラムが格納されている。

【0094】サーバマシン110での処理は、サーバマシンからクライアントマシンにコンピュータウィルスチェック要求を送信するまでの処理、すなわち、図8に示すコンピュータウィルスチェック要求プログラム、及び、図10に示すクライアントマシンから供給されたコンピュータウィルスチェック結果を集計するコンピュータウィルスチェック結果処理プログラムは、第1実施例と同一である。よって、図8に示すコンピュータウイルスチェック要求プログラム及び図10に示すコンピュータウイルスチェック結果処理プログラムの説明は省略する。

【0095】クライアントマシン120は、サーバマシンからのコンピュータウィルスチェック要求に応じてサーバマシン110のファイル装置111のプログラム領域112に格納されたコンピュータウィルスチェックプログラムにアクセスする。次に、本実施例のクライアントマシン120の構成を図面とともに説明する。図15に本発明の第3実施例のクライアントマシンのブロック

構成図を示す。同図中、図5と同一構成部分には同一符号を付し、その説明は省略する。

【0096】本実施例のクライアントマシン120では、ファイル装置121のプログラム領域122には、コンピュータウィルスチェックプログラムが保存されおらず、コンピュータチェック制御プログラムが保存されている。なお、上記のコンピュータウィルス制御チェックプログラムも他の実施例と同様、通信制御部を介して、または図示しないCD-ROMやフロッピーディスクなどの可搬型記録媒体に記録されてたものを読み取られ、上記ファイル装置121のプログラム領域122に格納されるものであり、プログラムの実行時には作業領域であるRAM25に格納され、そのプログラムに応じてCPU24により所定の処理が実行されるものである。

【0097】図16に本発明の第3実施例のクライアントマシンのコンピュータウィルスチェック制御プログラムの処理フローチャートを示す。クライアントマシン120ではサーバマシン110から自装置へのコンピュータウィルスチェック要求パケットを受信すると、コンピュータウィルスチェック制御プログラムを起動させ、サーバマシン110のファイル装置111のプログラム領域112に設定されたコンピュータウィルスチェックプログラムにアクセスし、コンピュータウィルスチェックプログラムを起動させる。(ステップS5-1)。

【0098】ステップS5-1で、サーバマシン110上のコンピュータウィルスチェックプログラムが起動されると、ファイル装置121のデータ領域22aに格納されたデータを順次、コンピュータウィルスパターン領域22dに格納されたコンピュータウィルスパターンと比較して一致するパターンを検索する。比較結果、コンピュータウィルスパターンと一致するデータが存在する場合には、ウィルスが存在すると判断して、ウィルスパターンの除去などを行うとともに、コンピュータウィルスパターンのバージョン情報、及び、検出したウィルスの情報を保持する。また、比較結果、コンピュータウィルスパターンと一致するデータが存在しない場合には、ウィルスは存在しないと判断して、チェックしたコンピュータウィルスパターンのバージョン情報、及び、ウィルスが存在しない旨の情報を保持する。

【0099】次に、コンピュータウィルスチェックプログラムのチェック結果を図6に示すようなサーバへの報告形式にまとめる(ステップS5-2)。クライアントマシン120は、ステップS5-2でのサーバマシンに記憶されたコンピュータウィルスチェックプログラムによるコンピュータウィルスのチェック後、図6に示すように自装置の属するグループID、自装置のメンバID、ウィルスチェック結果、コンピュータウィルスパターンのバージョン情報からなる結果報告情報を含むパケットを作成して、サーバマシンに通知する(ステップS

5-3)。

【0100】サーバマシン110は、クライアントマシン120からコンピュータウィルスのチェック結果を受信すると、図10に示すようにコンピュータウィルスチェック結果処理プログラムを実施する。本実施例によれば、サーバマシン110にコンピュータウィルスチェックプログラムを持ち、サーバマシン110からのコンピュータウィルスチェック要求に対してクライアントマシン120がサーバマシン110のコンピュータウィルスチェックプログラムにアクセスすることによりコンピュータウィルスのチェックを行うことにより、クライアントマシン120を全て同一バージョンのコンピュータウィルスパターンでチェックでき、サーバマシン110のコンピュータウィルスパターンを最新のバージョンにしておくだけで、全てのクライアントマシン120を最新のバージョンのコンピュータウィルスパターンでチェックできるので、クライアントマシン120をコンピュータウィルスから確実に防御できる。

【0101】また、クライアントマシン120は、コンピュータウィルスチェックプログラムを記憶する必要がないので、有効に使えるファイル領域が増大させることができ。なお、第1及び第3実施例では、サーバマシンはクライアントマシンの接続状態によらず、無条件にコンピュータウィルスチェック要求を行っていったが、所定の条件に従ってコンピュータウィルスチェック要求を行うことにより処理の自由度を向上させることもできる。

【0102】次に、所定の条件に従ってコンピュータウィルスチェック要求を行う実施例について説明する。まず、本実施例のサーバマシン110の構成を図面とともに説明する。図17に本発明の第4実施例のサーバマシンのブロック構成図を示す。同図中、図2と同一構成部分には同一符号を付し、その説明は省略する。

【0103】本実施例のサーバマシン210は、ファイル装置211に発信状況管理領域212を有する。発信状況管理領域212には、サーバマシン210でコンピュータウィルスチェックを行うクライアントマシンのコンピュータウィルスチェック要求発信予定日、各クライアントマシンを有効とする期限などを一括して管理する情報が格納される。

【0104】なお、クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 ... 3-n-1~3-n-mn、または、120と同一であるのでその説明は省略する。図18に本発明の第4実施例のサーバマシンの発信状況管理領域のデータ構成図を示す。

【0105】発信状況管理領域212は、サーバマシン210からのコンピュータウィルスチェックが有効となるクライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 ... 3-n-1~3-n-mn、または、120が属するグループIDを格納するグ

ループID領域、クライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 ... 3-n-1~3-n-mn、または、120のメンバIDを格納するメンバID領域、設定されたクライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 ... 3-n-1~3-n-mn、または、120のコンピュータウィルスチェック結果を送信する先のメールアドレスを格納するメールアドレス領域、コンピュータウィルスチェック要求の発信予定日を格納する発信予定日領域、コンピュータウィルスチェック要求を発信する期限を格納する発信期限領域から構成される。発信状況管理領域には、上記の情報を有効とするクライアントマシン数分だけ繰り返して格納される。

【0106】サーバマシン210は、図18に示す発信状況管理領域の情報に基づいてクライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 ... 3-n-1~3-n-mn、または、120にコンピュータウィルスチェック要求を発信する。図19に本発明の第4実施例のサーバマシンのコンピュータウィルスチェック要求処理プログラムの処理フローチャートを示す。

【0107】サーバマシン210では、コンピュータウィルス管理プログラムにより、図6に示すような要求スケジュールの参照して、設定されているグループ情報を順次取り出す（ステップS6-1, S6-2, S6-3）。次に、グループ情報中の発行日時情報領域に格納された発行日時情報を読み出して、現在日時と比較する（ステップS6-4）。ステップS6-4の比較結果、発行日時が現在日時であれば、要求スケジュールから参照したメンバ情報を読み出し、発信情報管理領域の対応する領域に設定する（ステップS6-5, S6-6）。

【0108】要求スケジュールをチェックし終わると（ステップS6-3）、次に、ステップS6-6で順次情報が設定された発信情報管理領域の情報を順次最終の情報まで参照する（ステップS6-7, S6-8）。このとき、まず、発信情報管理領域の期限領域に格納された期限を参照し、コンピュータウィルスチェックを行う期限が切れているか否かを判定する（ステップS6-9）。ステップS6-9での判定結果、コンピュータウィルスチェックを行う期限が切れている場合には、発信情報管理領域からそのメンバ情報を削除し、また、結果累積領域の対応するメンバ情報に期限切れである旨の情報を記録し、ステップS6-7に戻って、次のメンバ情報を参照する（ステップS6-10）。

【0109】また、ステップS6-9での判定結果、コンピュータウィルスチェックを行う期限が有効である場合には、次に、現在参照しているメンバ情報のクライアントマシン3-1-1~3-1-m1, 3-2-1~3-2-m2 ... 3-n-1~3-n-mn、または、120にアクセスし、クライアントマシン3-1-1~

$3 - 1 - m_1, 3 - 2 - 1 \sim 3 - 2 - m_2 \dots 3 - n - 1 \sim 3 - n - m_n$ 、または、120の接続状態を検出する(ステップS6-11)。

【0110】ステップS6-11での検出結果、現在参照しているクライアントマシン $3 - 1 - 1 \sim 3 - 1 - m_1, 3 - 2 - 1 \sim 3 - 2 - m_2 \dots 3 - n - 1 \sim 3 - n - m_n$ 、または、120が接続されていなければ、ステップS6-7に戻って、次のメンバ情報を参照する。また、ステップS6-11での検出結果、現在参照しているクライアントマシン $3 - 1 - 1 \sim 3 - 1 - m_1, 3 - 2 - 1 \sim 3 - 2 - m_2 \dots 3 - n - 1 \sim 3 - n - m_n$ 、または、120が接続されれば、コンピュータウィルスチェックを行うべきクライアントマシンであると判断できるので、発信情報管理領域の現在参照しているメンバ情報に設定されたメンバIDにコンピュータウィルスチェックを行う要求を行うためのコンピュータウィルスチェック要求パケットを送信し、発信情報管理領域の現在参照しているメンバ情報を削除して、ステップS6-7に戻って、次のメンバ情報を参照する(ステップS6-12)。

【0111】本実施例によれば、電源の切断、故障などによりサーバマシン210から接続できない、または、有効期限が切れて接続すべきでないクライアントマシンを判定して、「不在」として要求をスキップして、自動でコンピュータウィルスチェックを実行できる。

【0112】

【発明の効果】上述の如く、本発明の請求項1によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【0113】請求項2によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる等の特長を有する。

【0114】請求項3によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる等の特長を有する。請求項4によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端

末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる等の特長を有する。

【0115】請求項5によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる等の特長を有する。

【0116】請求項6によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行でき、また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができ、最新のウィルスパターンへの更新が容易に行える等の特長を有する。

【0117】請求項7によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【0118】請求項8によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるために、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる等の特長を有する。

【0119】請求項9によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を一括してチェックできる等の特長を有する。請求項10によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック

結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる等の特長を有する。

【0120】請求項11によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる等の特長を有する。

【0121】請求項12によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【0122】請求項13によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるために、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる等の特長を有する。

【0123】請求項14によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる等の特長を有する。請求項15によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる等の特長を有する。

【0124】請求項16によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる等の特長を有する。

【0125】請求項17によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータ

タウイルスパターンでウィルスチェックを行うことができる等の特長を有する。

【0126】請求項18によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【0127】請求項19によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる等の特長を有する。請求項20によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる等の特長を有する。

【0128】請求項21によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【0129】請求項22によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【0130】請求項23によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管

理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【0131】請求項24によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【0132】請求項25によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【0133】請求項26によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【図面の簡単な説明】

【図1】本発明の第1実施例のシステム構成図である。

【図2】本発明の第1実施例のサーバマシンのブロック構成図である。

【図3】本発明の第1実施例のコンピュータウィルスチェック要求スケジュールのデータ構成図である。

【図4】本発明の第1実施例の集計結果累積領域のデータ構成図である。

【図5】本発明の第1実施例のクライアントマシンのブロック構成図である。

【図6】本発明の第1実施例のクライアントマシンのコンピュータウィルスチェック結果領域のデータ構成図である。

【図7】本発明の第1実施例のクライアントマシンのコンピュータウィルスパターン領域のデータ構成図である。

【図8】本発明の第1実施例のコンピュータウィルスチ

エック要求プログラムの処理フローチャートである。

【図9】本発明の第1実施例のクライアントマシンのコンピュータウィルスチェックプログラムの処理フローチャートである。

【図10】本発明の第1実施例のサーバマシンのコンピュータウィルスチェック結果処理プログラムの処理フローチャートである。

【図11】本発明の第1実施例のグループ担当者に送信するコンピュータウィルスチェック結果一覧のフォーマットである。

【図12】本発明の第2実施例のサーバマシンのブロック構成図である。

【図13】本発明の第2実施例のコンピュータウィルスチェック要求プログラムの処理フローチャートである。

【図14】本発明の第3実施例のサーバマシンのブロック構成図である。

【図15】本発明の第3実施例のクライアントマシンのブロック構成図である。

【図16】本発明の第3実施例のクライアントマシンのコンピュータウィルスチェック制御プログラムの処理フローチャートである。

【図17】本発明の第4実施例のサーバマシンのブロック構成図である。

【図18】本発明の第4実施例のサーバマシンのファイル装置の発信状況管理領域のデータ構成図である。

【図19】本発明の第4実施例のサーバマシンのコンピュータウィルスチェック要求処理の処理フローチャートである。

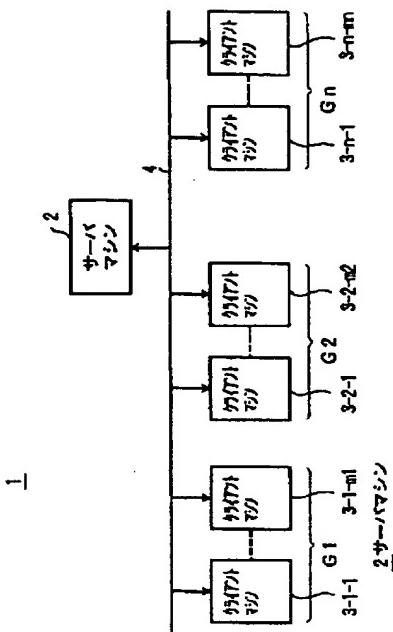
【符号の説明】

- | | |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 30 | 1 ネットワークシステム
2, 110 サーバマシン
3-1-1~3-1-m1, 3-2-1~3-2-m2
... 3-n-1~3-n-mn, 120 クライアントマシン |
| 40 | 1 1, 21 通信制御部
1 2, 22, 111, 211 ファイル装置
1 3, 23 入出力コントローラ
1 4, 24 CPU
1 5, 25 RAM
1 6, 26 ディスプレイ
1 7, 27 表示コントローラ
1 8, 28 キーボード
1 9, 29 キーボードコントローラ
2 0, 30 バス
1 2a, 22a データ領域
1 2b, 22b, 112 プログラム領域
1 2c コンピュータウィルスチェック要求スケジュール領域
1 2d 集計結果累積領域
2 2c コンピュータウィルスチェック結果領域 |

22d コンピュータウィルスパターン領域

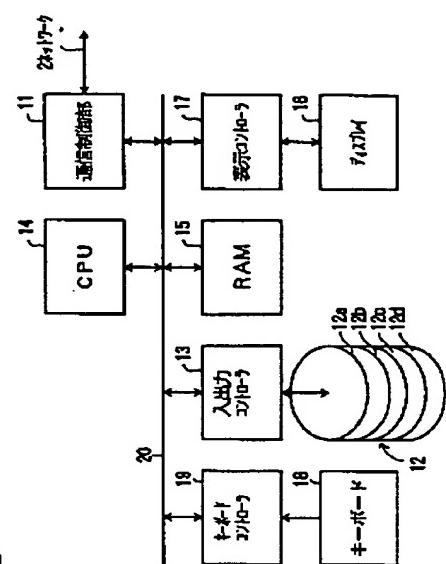
【図 1】

本発明の第1実施例のシステム構成図



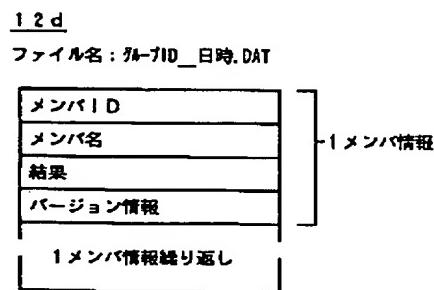
【図 2】

本発明の第1実施例のサーバマシンのブロック構成図



【図 4】

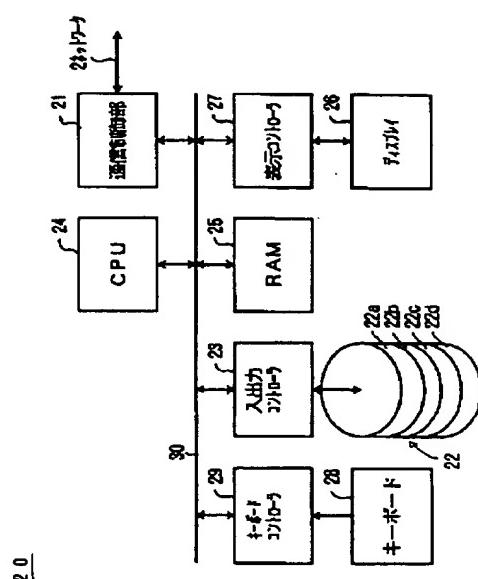
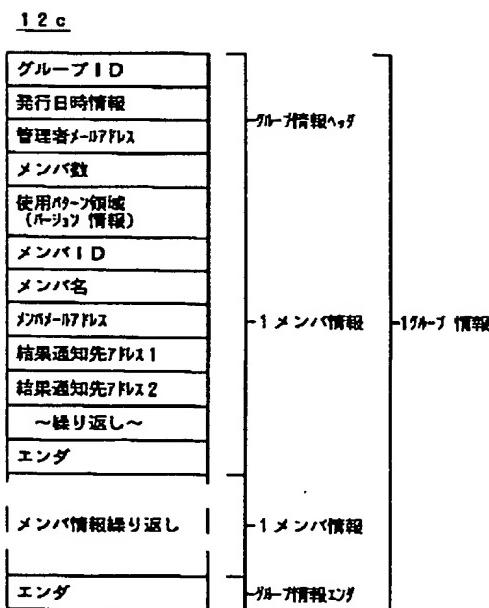
本発明の第1実施例の実験結果累積領域のデータ構成図



【図 5】

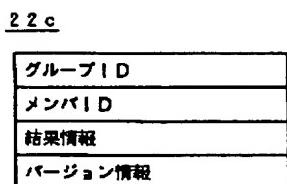
【図 3】

本発明の第1実施例のクライアントマシンのブロック構成図

本発明の第1実施例のコンピュータウィルスチェック
要求スケジュールのデータ構成図

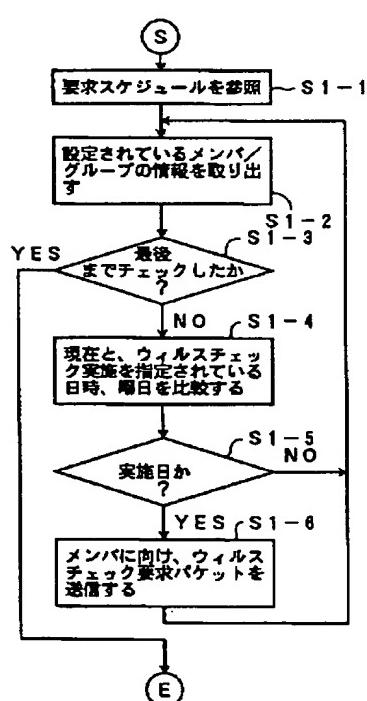
【図 6】

本発明の第1実施例のクライアントマシンのコンピュータ
ウィルスチェック結果領域のデータ構成図



【図 8】

本発明の第1実施例のコンピュータウィルスチェック
要求プログラムの処理フローチャート



【図 11】

本発明の第1実施例のグループ担当者に送信するコンピュータ
ウィルスチェック結果一覧のフォーマット

テキストファイル

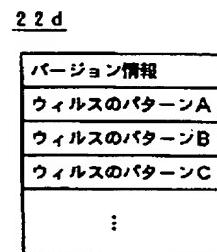
グループID:A
試行日時:97/07/07

[メンバ名: A氏]
使用パターン: V4+L4
結果: Normal end

[メンバ名: B氏]
使用パターン: V4+L4
結果: ウィルス+発見/除去しました

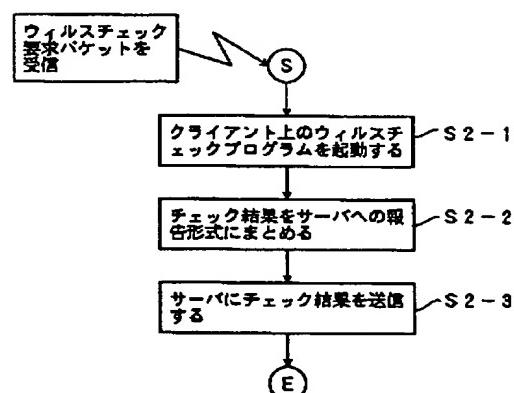
【図 7】

本発明の第1実施例のクライアントマシンのコンピュータ
ウィルスパターン領域のデータ構成図



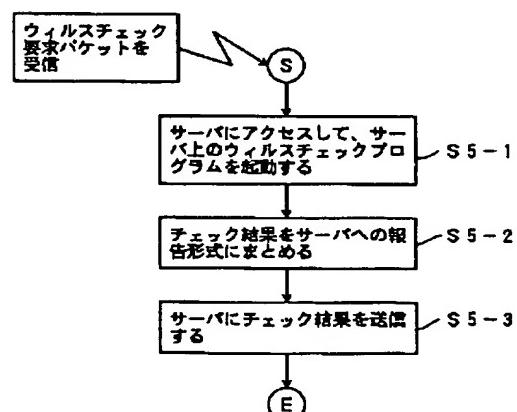
【図 9】

本発明の第1実施例のクライアントマシンのコンピュータ
ウィルスチェックプログラムの処理のフローチャート



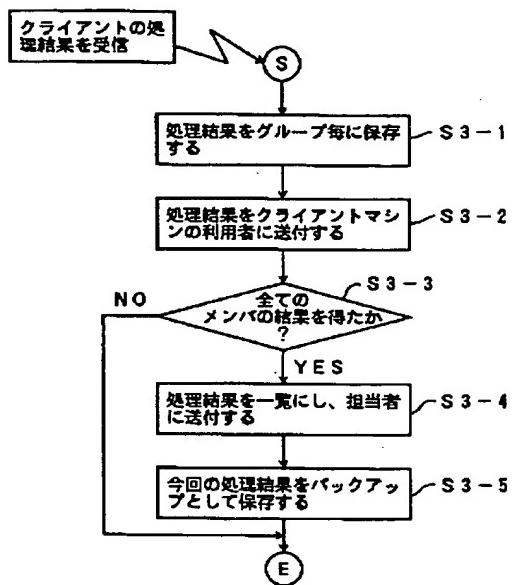
【図 16】

本発明の第3実施例のクライアントマシンのコンピュータ
ウィルスチェック制御プログラムの処理フローチャート



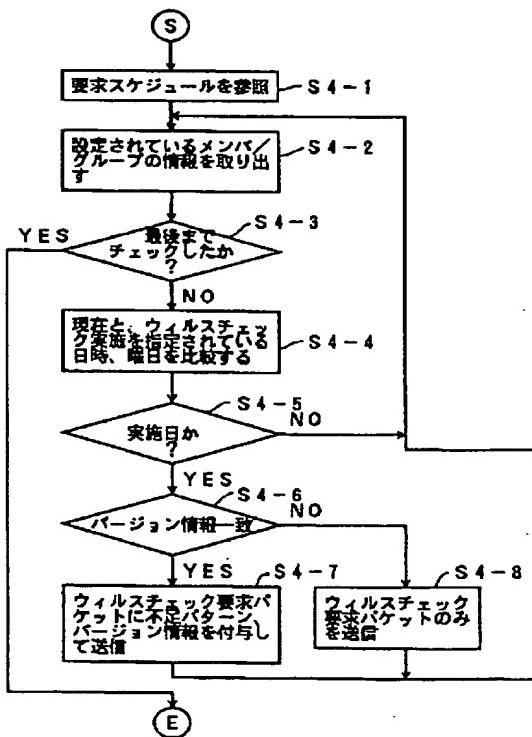
【図 10】

本発明の第1実施例のサーバマシンのコンピュータウィルス
チェック結果処理プログラムの処理フローチャート



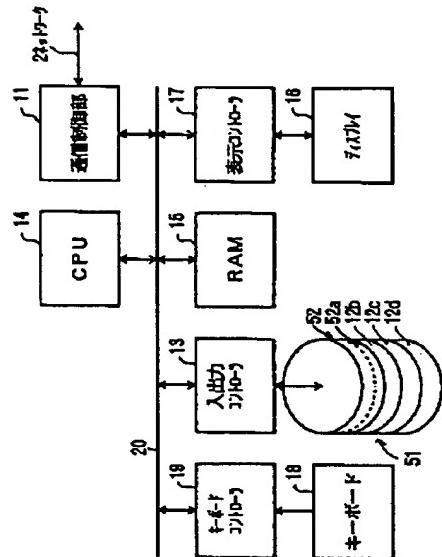
【図 13】

本発明の第2実施例のコンピュータウィルスチェック
要求プログラムの処理フローチャート



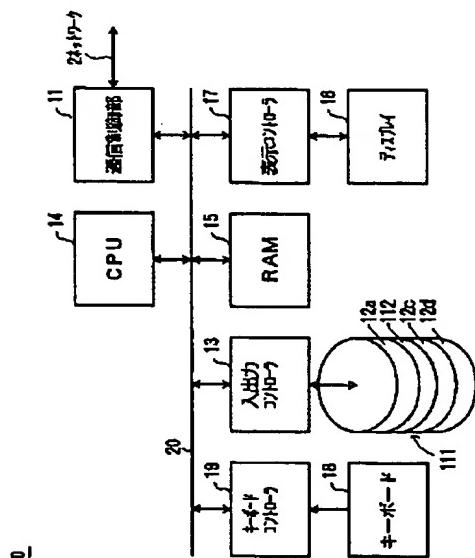
【図 12】

本発明の第2実施例のサーバマシンのブロック構成図



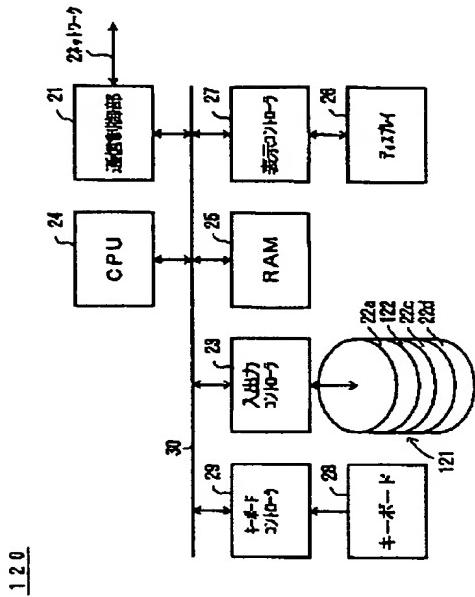
【図 14】

本発明の第3実施例のサーバマシンのブロック構成図



【図15】

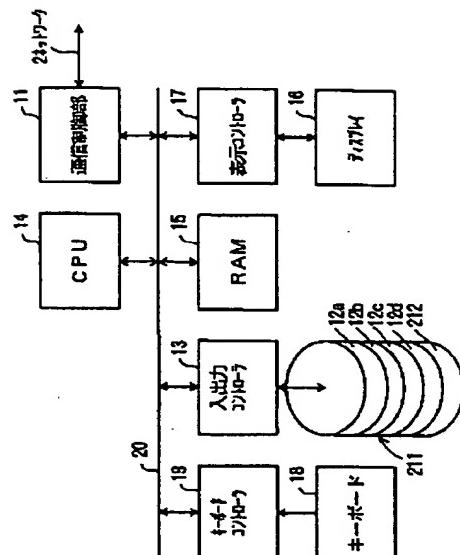
本発明の第3実施例のクライアントマシンのブロック構成図



120

【図17】

本発明の第4実施例のサーバマシンのブロック構成図



210

【図18】

本発明の第4実施例のサーバマシンのファイル

装置の発信状況管理領域のデータ構成図

発信状況管理構造

グループID	-1つの情報
メンバID	
メンバメールアドレス	
発信予定日	
発信期限	
繰り返し	

【図19】

本発明の第4実施例のサーバマシンのコンピュータウィルス
チェック要求処理の処理フローチャート

